INTEGRATION
ENGINEERING SAFETY MANAGEMENT

Crossrail Format and Process for Engineering Safety Justifications for Systems

Document Number: CRL1-XRL-O8-GPS-CR001-50004

Current Document History:

Revision:	Effective Date:	Author(s) ('Owner' in eB *)	Reviewed by: ('Checked by' in eB *)	Approved by:	Reason for Issue:
3.0	18/05/2016	Stephen James	Chi Wong	Jeremy Bates	2 Year Review

Previous Document History:

Revision	Prepared Date:	Author:	Reviewed by:	Approved by:	Reason for Issue
0.1	07-06-11	K. Harvey	C Bloxsome	M. Kilby	Internal review
1.0	22-06-11	K. Harvey	C Bloxsome	M. Kilby	Issued for implementation
2.0	16-05-12	K. Harvey	C Bloxsome	M. Kilby	Following peer review

Revision Changes:

Revision	Status / Description of Changes
3.0	2 Year Review; Reference documents updated and new format – minor (text) amendments

Contents

1 Purpose 4
2 Scope 4
3 Definitions 4
4 Background 5
5 Contents of Engineering Safety Justifications 5
5.1 Design Engineering Safety Justification 5
5.2 Engineering Safety Justification 8
6 Reference Documents 9

1 Purpose

The purpose of this document is to define the format and contents of Engineering Safety Justifications prepared to secure the safety acceptance of the various railway systems installed as part of the Crossrail Project.

2 Scope

Scope is limited to Design and Final Engineering Safety Justifications for the various railway systems on the central section of the Crossrail Project and which are to be prepared by the Crossrail Delivery Contractors.

It includes consideration of the requirement of the Railway Interoperability Regulations (RIRs) and the Regulation on common safety method for risk assessment and evaluation (CSM), which apply to the Crossrail Project.

This document does not apply to adjacent On Network Works where Network Rail Infrastructure Limited is the Infrastructure Manager.

3 Definitions

ALARP	As Low As Reasonably Practicable
BS	British Standards
CRL	Crossrail Limited
CSM	Common Safety Methods
DESJ	Design Engineering Safety Justification
EN	Euro Norm
ESJ	“Final” Engineering Safety Justification
ESM	Engineering Safety Management
LUL	London Underground Limited
NNTR	Notified National Technical Rule
NRIL	Network Rail Infrastructure Limited
PWHR	Project Wide Hazard Record
RIRs	Railway Interoperability Regulations.
SIL	Safety Integrity Level
TSI	Technical Specifications for Interoperability

4 Background

The requirement for Engineering Safety Justifications to be prepared for railway systems on the Crossrail Project is defined in:

- Crossrail Engineering Safety Management – System Safety Plan **[Ref 1]**.

This document also defines the approach for implementation of the RIRs and CSM Regulation on the Crossrail Project.

How this is implemented into the Crossrail Delivery Contracts is described in:

- Crossrail Delivery Contracts Standard Engineering Safety Management Requirements Specification **[Ref 2]**.

Engineering Safety Justifications are to be prepared for each of the Crossrail elementary systems as follows:

- Design Engineering Safety Justification (DESJ) – at the end of detailed design and before significant equipment procurement for the Delivery Contract;
- "Final" Engineering Safety Justification (ESJ) – following the successful completion of testing and commissioning to confirm the as-installed elementary system may be safely brought into service.

Where the scope of supply of the Delivery Contract includes more than one elementary system or that is complex, for example at an interface between two different signalling systems, it may be necessary for the Delivery Contractor to prepare several Engineering Safety Justifications in order to demonstrate safety and interoperability of the system.

5 Contents of Engineering Safety Justifications

5.1 Design Engineering Safety Justification

Design Engineering Safety Justification(s) **[Ref 4]** shall be a formal report(s) the content of which shall depend upon the extent that the scope of the justification is covered by the relevant TSI(s) / NNTR(s) as mandated by the RIRs. It shall include, but not limited to, the following evidence:

Part 1 – Introduction

- Including scope, definitions, abbreviations and references.

Part 2 - System Description

- A brief overview of the elementary system with reference to system design documentation, or other design deliverables generated by the Contract.

Part 3 – Engineering Safety Management System

- Principally to make reference to the current approved version of Contractor's System Safety Plan, which is a Contract safety deliverable
- Confirmation as to the adequacy of the implementation of the Contractor's System Safety Plan via reference to internal/external reviews and audits of engineering design, and including Suppliers and Sub-contractors.

Part 4 – Engineering Safety Analysis

- Confirmation and evidence that the engineering safety management has been carried out in conformance with the Contractors System Safety Plan which has been agreed with the Project Manager (CRL) and shown to be consistent with the Regulation on common safety method for risk assessment and evaluation[1] (CSM). This must demonstrate that the safety risks associated with the systems described in the DESJ have been correctly assessed and controlled to be tolerable and as low as reasonably practicable. Refer also to:
    - Crossrail Common Safety Methods Hazard Assessment Process **[Ref 3]**

Part 4a - Application of Codes of Practice

- Confirmation the elementary system(s) have been designed in compliance with the relevant codes of practice, standards and specifications (LUL, NRIL, BS, EN, TSIs, NNTRs etc.). With reference to design assurance documentation, or other design deliverables generated by the Contract[2].
- Identification of any non-compliances to the applicable codes of practice, standards or specifications and evidence the safety implications have been assessed and judged to be acceptable (i.e. ALARP).
- Confirmation significant assumptions in support of the design of the elementary system(s) have been identified and the safety implications assessed and judged to be acceptable (i.e. ALARP).
- Evidence that the safety requirements have been achieved, non-compliances identified and safety implications assessed and judged to be acceptable (i.e. ALARP). With reference to the Safety Requirements Specification and the Safety Integrity Level (SIL) Requirements Report which are Contract safety deliverables.

Part 4b - Comparison with Similar (Reference) Systems

- Evidence of relevant, previous and proven use, and safety approvals of components, equipment and systems with reference to the Product Breakdown Structure which is a Contract safety deliverable. Where “reference systems” are claimed as per the Common Safety Methods this should be clearly identified.
- Confirmation that components, equipment and systems are to be procured from reputable Suppliers / Manufacturers and with reference to the evidence provided in the Product Breakdown Structure. Where unproven Suppliers / Manufacturers are proposed this should be highlighted and justified.

---

[1] The Contractor can only demonstrate compliance with their own System Safety Plan, it is the responsibility of CRL to ensure this Plan discharges and activities required to assure compliance with the CSM regulation. An Independent Assessment Body (AsBo) appointed by CRL will provide assurance under the Regulations that the CSM Regulation has been complied with, and will issue a Safety Assessment Report to confirm this.

[2] Where the scope of the DESJ is covered, or partly covered by the relevant TSIs/NNTR(s) then the evidence of compliance of these parts will be provided by the NoBo/DeBo appointed by CRL:

- Intermediate Statement of Verification to the relevant TSIs & NNTRs
- Technical File containing the evidence specified in RIR Schedule 6

This evidence will be made available by CRL, who are the Contracting Entity under the RIRs.

- Reference to safety analyses of any claims made for cross-acceptance where the Crossrail application and/or environment may be fundamentally different to the claimed reference system(s).
- Reference to the CRL approved Product Safety Cases prepared by the Delivery Contractor where cross-acceptance has not easily feasible and use on Crossrail Project has needed to be pre-authorised.

Part 4c – Explicit Risk Estimation

- Provide, or make reference to, any explicit risk estimation which has been undertaken.
- Summary and discussion of the main safety risks associated with the elementary system(s) and how these risks are mitigated. With reference to the Project Wide Hazard Record which is the principle hazard management tool and a Contract safety deliverable. For further information refer to Technical Note on the use of Project Wide Hazard Review in Engineering Safety Management Process **[Ref 5].**
- Highlight any particular safety issues or concerns and how these risk have been managed.

Part 5 - Supporting Engineering Safety Evidence

- List of safety documentation and Contract Safety deliverables prepared and issued, and giving their approval status. Including, but not limited to:
  - Details of safety related workshops (e.g. HAZIDs, HAZOPs) carried out.
  - Details of any safety analyses and assessments undertaken.
  - Other relevant documentation.

Part 6 – Safety Constraints and Assumptions

- List and explanation of any safety operating constraints relevant to the elementary system(s) (e.g. functional, operational, physical parameters which are vital to safe operation).
- List and explanation of any minimum operating requirements which must be met to assure the safety of the continuing operation of the elementary system(s) (e.g. level of degraded operation with failed components / equipment; redundant equipment allowed out of service for maintenance).
- List and explanation of any safety related assumptions, or other safety issues, to be brought to the attention of future operators and maintainers of the elementary system(s).

Part 7 - Conclusions

- Judgement that design has been carried out in accordance with good engineering safety practice and the functional, technical and safety requirements of the Contract.
- Judgement that all safety requirements have been met, or, if not, safety risks managed and controlled to ALARP
- Judgement that the design may be operated and maintained such that the risks are managed and controlled to ALARP

5.2 Engineering Safety Justification

The "Final" Engineering Safety Justification shall be an update to the Design Engineering Safety Justification including the following additional information:

- Update of the evidence already included and referenced in the Design Engineering Safety Justification.[3]
- Confirm the successful completion of testing and commissioning such that the safety requirements are achieved and the elementary system(s) may be safely brought into service. With reference to the Safety Requirements Specification which is a Contract safety deliverable.
- Identify and discuss any safety concerns, or other issues, observed during testing and commissioning and how these were resolved.
- Identify and justify the safety of any design, or other, changes implemented as a consequence of testing and commissioning.

[3] Where the scope of the ESJ is covered, or partly covered by the relevant TSIs/NNTR(s) then the evidence of compliance of these parts will be provided by the NoBo/DeBo appointed by CRL:

- Certificate of Conformity to the relevant TSIs & NNTRs
- Technical File containing the evidence specified in RIR Schedule 6

This evidence (updated from the DESJ) will be made available by CRL, who are the Contracting Entity under the RIRs.

6 Reference Documents

Ref:	Document Title	Document Number:
1.	Engineering Safety Management System Safety Plan.	CRL1-XRL-O7-GST-CR001-00001
2.	Crossrail Delivery Contracts Standard Engineering Safety Management Requirements Specification	CRL1-XRL-O8-GPD-CRG03-50001
3.	Crossrail Common Safety Methods Hazard Assessment Process	CRL1-XRL-O8-GPS-CR001-50003
4.	Requirements for the Creation, Format and Provision of a Design Engineering Safety Justification (DESJ)	CRL1-XRL-O8-GPS-CR001-50025
5.	Technical Note on the use of Project Wide Hazard Review in Engineering Safety Management Process	CRL1-XRL-O8-GPS-CR001-50024